

Appl. No. 09/619,633
Amdt. Dated: September 27, 2004
Reply to Office Action of: 03/25/2003

Amendments to the Specification

Please replace the paragraph on Page 2 beginning on line 21 and continuing to Page 3, line 7 with the following amended paragraph:

In accordance with this invention there is provided a method for generating a shared secret value between entities in a data communication system, one or more of the entities having a plurality of members for participation in the communication system, each member having a long term private key and a corresponding long term public key, the method comprising the steps of:

- (a) generating an ~~entity long term private key and corresponding~~ entity long term public key for each entity by combining the long term ~~private and~~ public keys of each members of the entity.
- (b) ~~generating~~ a short term private and a corresponding short term public key for each of the members;
- (c) ~~exchanging~~ making said short term public key ~~of the~~ available to members within an entity;
- (d) for each member:
 - (i) computing an intra-entity shared key by mathematically combining said short term public keys of each said member;
 - (ii) computing an intra-entity public key by mathematically combining its short-term private key, the long term private key and said intra-entity shared key;
- (e) for each entity combining intra-entity public keys to derive a group short-term public key;
- (f) each entity ~~transmitting~~ making its intra-entity shared key and its ~~group short-term public key~~ entity long term public key available to said other entities; and
- (g) each entity computing a common shared key K by combining its group short term public key, with the intra-entity shared key, and an entity long term public key received from the other entity.

Appl. No. 09/619,633
Amdt. Dated: September 27, 2004
Reply to Office Action of: 03/25/2003

Please replace the paragraph on Page 3, beginning on line 17 with the following amended paragraph:

Referring to figure 1, a schematic diagram of a communication system is shown generally by numeral 10. The system 10 includes a first entity A (12) and a second entity (B) that exchange data over a communication channel 16. Each of the entities A and B include members $A_1, A_2 \dots A_n$, and $B_1, B_2 \dots [B_n] B_m$, respectively. For convenience, the embodiment described has two members A_1, A_2 and B_1, B_2 although it will be appreciated that typically each entity will have several members. It is assumed the entities A and B include processors for performing cryptographic operations and the like. The members A_1, A_2 may for example be a first group of users on a local area network (LAN) that wish to communicate securely with a second group of users B_1, B_2 on a second LAN or even on the same LAN. In either case the computations may be performed for the entities A (12) and B (14) by for example a LAN server 18 or the like, provided that each member has its own secure boundary.

Please replace the paragraph on Page 4 beginning on line 21 with the following amended paragraph:

Next, member A_1 computes $r = x_1P + x_2P$ and similarly, entity member A_2 computes $r = x_2P + x_1P$. Thus, establishes an intra-entity shared key available and containing a contribution from each member of the entity.